УДК 004.056.53

К. В. Пугачева
Т. Г. Кирилащук

КОРЕЛЯЦІЙНИЙ АНАЛІЗ ПОДІЙ БЕЗПЕКИ (SIEM) ДЛЯ ВИЯВЛЕННЯ ЕТАПУ «LATERAL MOVEMENT» НА ОСНОВІ СИНТЕЗУ ТЕХНІЧНИХ ТА ОРГАНІЗАЦІЙНИХ ДАНИХ

Вінницький національний технічний університет

Анотація

У роботі досліджено специфіку виявлення етапу горизонтального переміщення (Lateral Movement) в умовах використання зловмисниками легітимних інструментів адміністрування (Living off the Land). Проаналізовано ключові недоліки класичних правил кореляції SIEM-систем порівняно з контекстно-орієнтованими підходами, зокрема нездатність розрізняти дії зловмисників та легітимних адміністраторів при використанні валідних облікових записів. Визначено проблему «контекстної сліпоти» та «втоми від тривог» (Alert Fatigue), що виникає через високий рівень помилкових спрацювань і ускладнює роботу центрів моніторингу безпеки (SOC). На основі аналізу технік MITRE ATT&CK запропоновано метод оптимізації правил кореляції, що базується на синтезі технічних подій із організаційним контекстом (роль користувача, критичність активу, часові рамки) та динамічній оцінці ризику.

Ключові слова: *SIEM, Lateral Movement, кореляційний аналіз, синтез даних, контекстно-орієнтований підхід, SOC, Living off the Land.*

Abstract

The paper examines the specifics of detecting the Lateral Movement stage under conditions where attackers use legitimate administrative tools (Living off the Land). Key shortcomings of traditional SIEM correlation rules are analyzed in comparison with context-oriented approaches, particularly their inability to distinguish malicious activity from legitimate administrator actions when valid credentials are used. The study identifies the problems of "context blindness" and "alert fatigue," which arise due to a high rate of false positives and significantly complicate the work of Security Operations Centers (SOC). Based on an analysis of MITRE ATT&CK techniques, a method for optimizing correlation rules is proposed. This method is based on synthesizing technical events with organizational context (user role, asset criticality, time frames) and on dynamic risk assessment..

Keywords: SIEM, Lateral Movement, correlation analysis, data synthesis, context-oriented approach, SOC, Living off the Land.

Вступ

Для моніторингу безпеки та управління інцидентами в корпоративних мережах стандартними стали SIEM-системи, що збирають величезні масиви даних з різних джерел. Для виявлення складних цілеспрямованих атак, в яких зловмисники переходять до етапу горизонтального переміщення (Lateral Movement). Дедалі частіше для реалізації цієї частини стали використовувати техніки «Living off the Land» (LotL), маскуючи свої дії під легітимну активність системних адміністраторів за допомогою стандартних інструментів ОС (PowerShell, WMI, RDP).

Актуальність теми зумовлена тим, що методи кореляції події стають неефективними, якщо зловмисники використовують скомпроментовані валідні облікові записи, оскільки опираються виключно на технічні сигнатури та статичні правила. Відсутність врахування бізнес-контексту призводить до високого рівня помилкових спрацювань (False Positives). Це перевантажує аналітиків SOC (Security Operations Center) та знижує швидкість реагування на реальні загрози.

Метою даної роботи є підвищення ефективності виявлення прихованого переміщення зловмисника в мережі шляхом розробки методу кореляційного аналізу, що базується на синтезі технічних подій безпеки та контекстних організаційних даних.

Результати дослідження

1. Проблематика виявлення Lateral Movement

Lateral Movement – це процес, під час якого зловмисники глибоко проникають в заражену систему для того, аби контролювати додаткові системи або отримати доступ до конфіденційних даних і вразливостей. [1]

Аналіз сучасних підходів до виявлення горизонтального переміщення зловмисника дозволив виділити низку критичних проблем, які ускладнюють своєчасне реагування на інциденти:

– Несумісність форматів даних для автоматизованого аналізу. За допомогою стандартних хасобів логування Windows події зберігаються у бінарному форматі EVTX. Цей формат є оптимізованим для зберігання, але непридатним для прямої обробки алгоритмами машинного навчання, які потребують структурованих табличних даних (CSV). Це створює технічний бар'єр на етапі збору та попередньої обробки інформації, вимагаючи розробки спеціалізованих інструментів конвертації та парсингу.

– Складність визначення еталону «нормальної поведінки». Для того, аби коректно виявляти аномалії важливим є формування чистої навчальної вибірки (Baseline). Необхідність гарантій, що дані, зібрані для тренування моделі, відображають виключно легітимну діяльність користувачів є проблемою. Оскільки наявність будь-яких прихованих атак або «шуму» у навчальному наборі може призвести до хибного навчання моделі та нездатності розпізнавати реальні загрози.

– Прості сигнатурні методи є неефективними проти поведінкових аномалій. При Lateral Movement дії зловмисників часто не мають чітких сигнатур, а проявляються як статистичні відхилення. Класичні засоби не здатні ефективно оцінювати кластерну приналежність та щільність розподілу подій, тобто аномально низьку щільність у просторі ознак.

– Аналіз даних потребує гнучкого інструментарію. Вирішення задач кластеризації та статистичного аналізу вимагає використання мов програмування з широким спектром бібліотек для Data Science (таких як Python), що дозволяє реалізувати складні алгоритми обробки даних, недоступні в "коробкових" продуктах. [2]

Отже, основна проблематика полягає у необхідності автоматизованого перетворення сирих логів Sysmon у придатний для аналізу формат та застосуванні математичних методів для виявлення аномалій, що відхиляються від моделі легітимної поведінки

2. Як працюють стандартні правила SIEM. Аналіз неефективності класичних методів SIEM

SIEM (Security Information and Event Management) – це інструмент кіберзахисту, який створений для того, щоб компанії могли швидко виявляти потенційні загрози та усувати їх ще до того, як вони зашкодять бізнес-процесам. Така система допомагає фахівцям з інформаційної безпеки відстежувати підозрілу активність і нестандартну поведінку користувачів.

На базовому рівні всі системи SIEM виконують такі функції:

– Збір та управління журналами. Інформацію про події з різних джерел в IT-інфраструктурі компанії збирає SIEM та аналізує в реальному часі.

– Кореляція подій. Аналітичні інструменти швидко виявляють складні патерни у даних, що допомагає швидко ідентифікувати потенційні загрози.

– Моніторинг інцидентів. У єдиній панелі управління системи SIEM централізують аналітичні дані. Там команди безпеки можуть відстежувати активність, сортувати сповіщення, виявляти загрози та оперативно реагувати або усувати їх.

– Відповідність. Системи SIEM є ефективним інструментом для перевірки відповідності стандартам PCI DSS, ISO, GDPR, HIPAA та іншим у реальному часі. [3]

Класичні системи SIEM ефективно вирішують задачі відповідності стандартам та виявлення базових загроз, проте є неефективними при протидії цілеспрямованим атакам (APT) на етапі горизонтального переміщення. Головною причиною цього є обмеженість статичних правил кореляції, які спираються на детерміновану логіку. Наприклад, фіксація кількості невдалих спроб входу за хвилину. У сучасності ж зловмисники використовують тактику «Low and Slow», розтягуючи свої дії у часі.

Класичний метод кореляції аналізує подію ізольовано від бізнес-логіки організації, фіксуючи лише технічний факт успішного входу користувача на сервер або запуску процесу. Система не враховує критично важливі метадані, такі як відповідність часу активності робочому графіку співробітника, його посадові обов’язки або типовість використовуваної IP-адреси. Без синтезу технічних подій із цим організаційним контекстом SIEM-система не здатна відрізнити легітимний сеанс адміністратора від дій зловмисника, який оперує вкраденою сесією.

Компенсація недоліків спробою підвищенням чутливості правил призводить до лавиноподібного зростання кількості помилкових спрацювань (False Positives) на легітимні дії персоналу. Це спричиняє феномен «втоми від тривог» (Alert Fatigue) у аналітиків SOC (Security Operations Center), коли реальні інциденти горизонтального переміщення Lateral Movement розсіюються у загальному шумі або ігноруються.

3. Застосування контекстно-орієнтованого підходу (Context-Awareness) для збагачення подій

SIEM-систем

Для того, аби подолати обмеження класичних методів кореляції та усунути проблему «сліпоти до контексту» пропонується застосування контекстно-орієнтованого підходу (Context-Awareness). Цей підхід у трансформації процесу обробки даних: перехід від аналізу ізольованих технічних подій до аналізу багатовимірних інформаційних об'єктів. Підхід реалізується через механізм збагачення даних (Data Enrichment), який передбачає автоматичне доповнення лог-файлів метаданими з зовнішніх джерел, коли ті надходять до системи SIEM.

Ключовим вектором збагачення є контекст користувача (Identity Context), який формується через інтеграцію з кадровими системами та Active Directory. Такий спосіб дозволяє враховувати роль, відділ та статус співробітника, виявляючи нетипову активність (доступ маркетолога до баз даних) та ознаки компрометації легітимних акаунтів, зокрема складні атаки на інфраструктуру аутентифікації, такі як Golden Ticket. [4]

Контекст активів (Asset Context), що визначає критичність вузлів мережі на основі даних CMDB. Він дозволяє динамічно пріоритезувати інциденти, автоматично підвищуючи вагу подій на критичних серверах (контролери домену, фінансові системи) порівняно з тестовими сегментами.

Третім шаром є ситуаційний та часовий контексти (Environmental & Temporal Context), які порівнюють поточну подію з історичним профілем поведінки (Baseline). Аналіз відхилень у часі входу, геолокації чи обсягах даних перетворює SIEM на інтелектуальну систему, здатну виявляти приховані маневри зловмисника на основі поведінкових аномалій, а не лише жорстких правил.

4. Оптимізація правил кореляції SIEM шляхом синтезу даних

Після проведено аналізу пропонується вдосконалена модель правил кореляції, яка полягає у переході від спрощеної бінарної логіки до динамічної оцінки ризику на основі синтезованих даних. На відміну від традиційного підходу, де інцидент створюється автоматично при досягненні певного порогу подій, оптимізована модель використовує алгоритм зваженого ризику, де технічна вага події коригується коефіцієнтом аномальності контексту.

Якщо певну адміністративну дію виконує профільний фахівець у робочий час на дозволеному сегменті мережі, коефіцієнт ризику мінімізується, і система не генерує тривогу. Виконання тієї ж дії користувачем із невідповідною роллю, у неробочий час або на критично важливому сервері, призводить до експоненціального зростання показника ризику та створення пріоритетного інциденту.

Такий підхід дозволяє автоматично відфільтровувати легітимну активність, що раніше створювала інформаційний шум, та фокусувати увагу аналітиків SOC виключно на подіях з високим ризик-балом. Це значно підвищує точність виявлення етапу Lateral Movement, навіть при використанні зловмисником легітимних інструментів, оскільки його поведінковий патерн неминуче відхилятиметься від нормального профілю співробітника.

Запропонований метод синтезу технічних та організаційних даних дозволяє вирішити проблему високого рівня помилкових спрацювань у сучасних SIEM-системах, перетворюючи процес моніторингу з пасивного накопичення логів на проактивний інструмент виявлення цілеспрямованих атак.

Висновки

У роботі проаналізовано проблематику виявлення складних цілеспрямованих атак (APT) на етапі горизонтального переміщення (Lateral Movement). Встановлено, що класичні методи моніторингу на базі SIEM-систем, які спираються на статичні правила кореляції та сигнатурний аналіз, втрачають ефективність в умовах використання зловмисниками технік «Living off the Land» та валідних облікових записів. Головним недоліком існуючих підходів визначено «сліпоту до контексту», що призводить до високого рівня помилкових спрацювань (False Positives) та перевантаження аналітиків SOC.

Основним науковим результатом роботи є обґрунтування та розробка методу удосконалення правил кореляції шляхом синтезу технічних подій безпеки з організаційним контекстом. Запропонований підхід передбачає динамічне збагачення логів даними про роль користувача (Identity Context), критичність активів (Asset Context) та історичну поведінку (Temporal Context).

Доведено, що перехід від бінарної логіки виявлення до моделі динамічної оцінки ризику (Risk Scoring) дозволяє автоматично відсіювати легітимну адміністративну активність. Це забезпечує підвищення точності виявлення прихованих маневрів зловмисника та трансформує систему SIEM з інструменту пасивного логування в засіб проактивного захисту корпоративної інфраструктури.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. What is that Lateral Movement? [Електронний ресурс]. – Режим доступу: https://www.trendmicro.com/en/what-is/data-breach/lateral-movement.html (дата звернення: 15.02.2026).
2. Жердєв М. К., Гнатюк С. О. Методи виявлення цілеспрямованих кібератак в інформаційно-комунікаційних системах [Електронний ресурс]. – Режим доступу: https://ela.kpi.ua/server/api/core/bitstreams/bede804a-c6d4-44b0-bc9d-adfc97f5279d/content (дата звернення: 15.02.2026).
3. Що таке SIEM: простими словами про важливий інструмент кіберзахисту [Електронний ресурс]. – Режим доступу: https://gigacloud.ua/articles/shcho-take-siem-prostymy-slovamy-pro-vazhlyvyy-instrument-kiberzakhystu/ (дата звернення: 15.02.2026).
4. Melnyk A., Galchynsky L. Active Directory Golden Ticket Attack Detection // International Research Journal of Engineering and Technology (IRJET). – 2023. – Vol. 10. – P. 750–759 [Електронний ресурс]. – Режим доступу: https://gigacloud.ua/articles/shcho-take-siem-prostymy-slovamy-pro-vazhlyvyy-instrument-kiberzakhystu/ (дата звернення: 15.02.2026).

Крістіна Вікторівна Пугачева – студентка групи 2КІТС-24б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: kristipref@gmail.com;

Науковий керівник: Тетяна Генадіївна Кирилащук – асистент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail: kgt0998@gmail.com.

Kristina V. Puhacheva – student of group 2KITS-24b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: kristopref@gmail.com;

Supervisor: Tatiana G. Kyrylashchuk – Assistant of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia, e-mail: kgt0998@gmail.com.